# J3

## PRECISE JAMMING SYSTEM

# User Manual

V1.0

# Reading Tips

This manual applies to the UAV radio countermeasure equipment developed and produced by the company. The manual provides comprehensive specifications, functional design, structure and specification requirements of the system, as well as installation, deployment, and operational requirements, serving as an operational guide for end users.

## Symbol Legend

| | |
|---|---|
| | Supplementary Notes: Additional explanations and annotations to the main text of the manual. |
| | Safety Notices: Important operational warnings and risk prevention guidelines for users. |
| | DANGER: Indicates imminent hazards which, if not avoided, will result in death or serious injury and major property damage. |

## Manual Usage Recommendations

1. Before using the product, please read this manual thoroughly. Retain this manual for future reference to address any operational inquiries.
2. All photographs, graphics, charts, and illustrations in this manual are for explanatory purposes only and may differ from the actual product. Refer to the physical product for exact specifications. The company reserves the right to update this manual due to product version upgrades or other requirements, with the latest electronic version to be distributed to users.
3. The company recommends using this manual under the guidance of qualified personnel.

# Safety Notice

Before using the product, please carefully read the following precautions and operate the product correctly as required.

## Installation Precautions

### Environmental Requirements

Do not install or store the product in any of the following locations:

- Extreme environments: places where temperatures exceed the range of -40°C to +55°C or where frost may form.
- Near strong electromagnetic interference sources or equipment with large current fluctuations.
- Areas with flammable, explosive, corrosive gases or dust.
- Damp or water-exposed areas. Liquid ingress may cause electric shock or fire hazards.

### Operational Guidelines

- Only qualified personnel or designated maintenance staff may open the chassis.
- All antennas must be fully connected and tightened according to the labels. Powering on the device without antennas installed is strictly prohibited.

## Usage Precautions

### Power and Electrical Safety

- Use only the specified AC 110 V–220 V power supply.
- Do not pull or bend the power cord. Avoid crushing or twisting it, and stop using it if damaged.
- Do not operate the equipment during thunderstorms. Avoid touching power lines or device connectors during lightning to prevent electric shock.

- Always unplug the power cord before moving the device.
- Do not touch the power plug with wet hands.
- When unplugging the power cord, hold the plug body firmly.

## Operational Risk Warnings

- If abnormal conditions such as smoke, unusual noises, or burning smells occur, shut off power immediately and contact our after-sales service department.
- Do not install any software unrelated to the software platform; system issues caused by such software are not covered under warranty.
- Do not connect unauthorized USB drives or external hard drives to avoid malware infection. Do not delete server files arbitrarily, change the system time, or shut down or restart the server without authorization.
- Unauthorized personnel are prohibited from disassembling the device to avoid damaging internal components or compromising your rights. If the device malfunctions during use, contact our after-sales service department.

## Regulatory Compliance

- This device may cause radio interference during operation. Users must take feasible measures to mitigate such interference.
- If suspected interference occurs with civil-aviation or military frequencies, stop using the device immediately, investigate the cause, and report the incident.

# Table of Contents

READING TIPS I

Symbol Legend I

Manual Usage Recommendations I

SAFETY NOTICE II

Installation Precautions II

Usage Precautions II

1 PRODUCT INTRODUCTION 3

1.1 Main Functions 3

1.2 Product Appearance 4

1.3 Ports and Antenna Connector 5

1.4 Mechanical Characteristics 7

2 EQUIPMENT DEPLOYMENT PREPARATION 8

2.1 Site Selection 8

2.2 Installation Methods 9

3 DEPLOY THE EQUIPMENT 11

3.1 Connect Antennas 11

3.2 Connect with Detection Device 11

3.3 Connect Fan 13

3.4 Connect Power Supply 13

4 DRONE DEFENSE SOFTWARE PLATFORM 14

4.1 Log in to the System 14

4.2 Main Interface 15

4.3 Check Detection Information 20

4.4 Drone Jamming 21

4.5 Enable Unattended Function 22
4.6 Check the Events 23
4.7 Mark Danger WiFi Drones 23
4.8 Manage the Whitelist/Blacklist 24
4.9 Check the Statistic Report 25
4.10 Check the Device Status 26
4.11 Change Password 26
4.12 Manage Users 26

**5 EQUIPMENT MAINTENANCE 28**

5.1 Routine Maintenance 28
5.2 Basic Troubleshooting 28

**6 PACKAGING, TRANSPORTATION AND STORAGE 30**

6.1 Packaging 30
6.2 Transportation 30
6.3 Storage 30

# 1 Product Introduction

J3 is a stationary defense priority product, which is designed with the fusion of multiple jamming technologies, supporting the effective jamming of the drone's graphic transmission, remote control and navigation signals by means of wide-band, narrow-band low-power precise jamming and navigation defense to make it return or land. It features low average transmission power, low environmental impact and high defense reliability.

J3 requires integration with detection device to achieve drone detection and defense capabilities through the low-altitude drone defense software platform.

## 1.1 Main Functions

**Precise Jamming**

Uses unique narrow-band, low-power precision jamming technology to target single or multi-drones while no affected on other drones.

**Full Range Coverage**

Adopting omni-directional antenna array, the jamming range covers 360°, realizing omni-directional and dead-angle-free jamming of drones.

**Network Coordination**

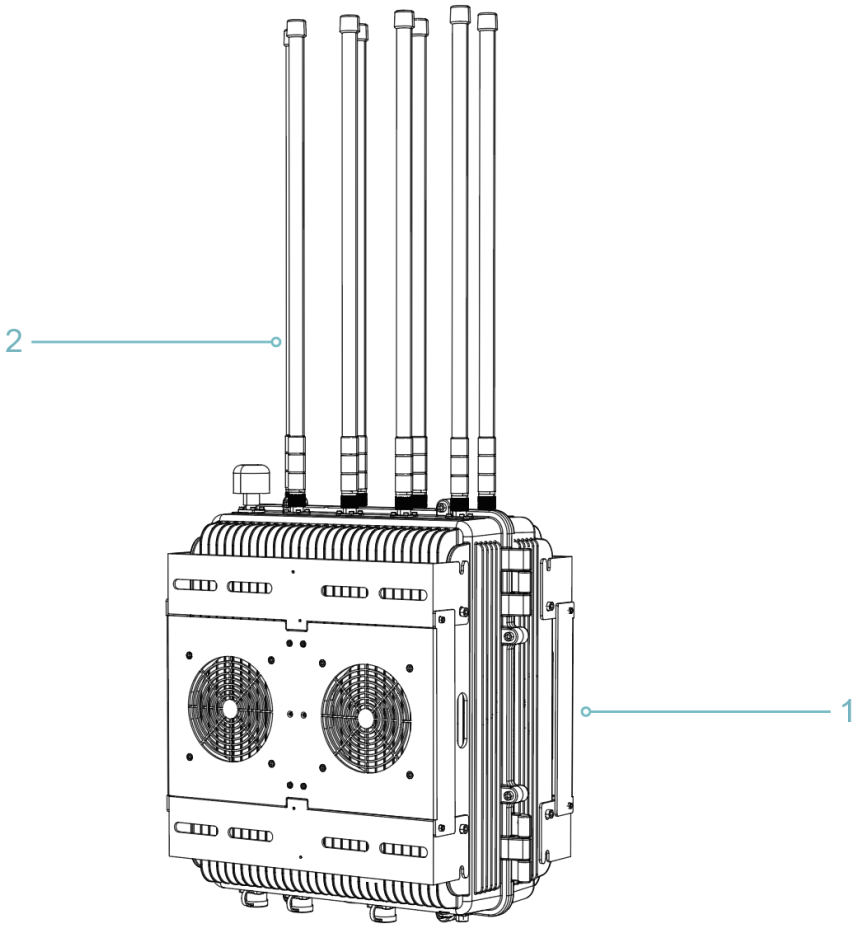
Support network coordination with other radar, optoelectronic and radio detection equipment to realize countermeasures against conventional/non-conventional targets.

**Comprehensive Defense**

Narrow-band, frequency-hopping, low-power precise jamming combined with wide-band, high-power jamming to achieve comprehensive drone defense.

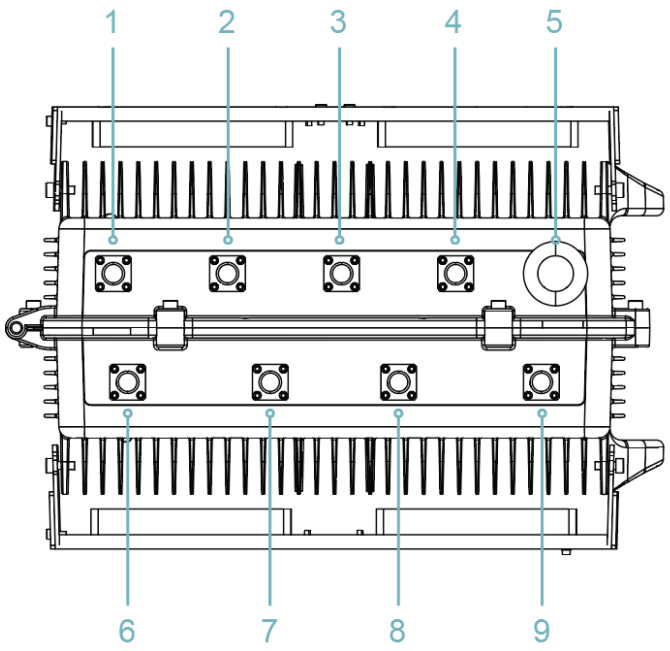
## 1.2 Product Appearance

The equipment appearance is shown as follows:



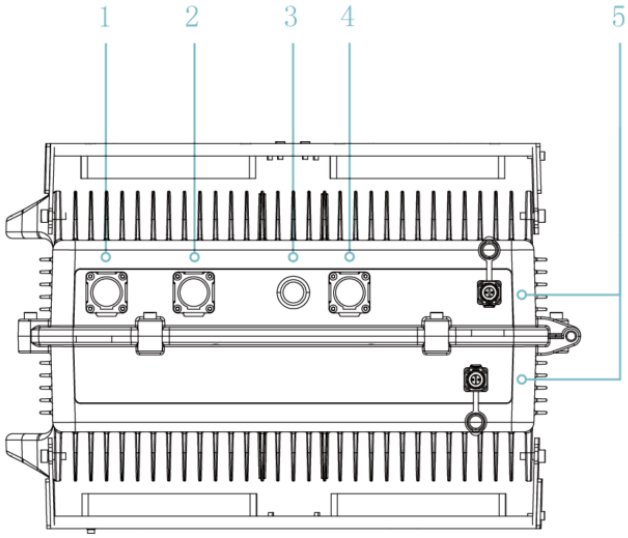

1. Main unit
2. Antennas

## 1.3 Ports and Antenna Connector




| Position | Description | Label | Connector Type |
|---|---|---|---|
| 1 | 1.5GHz transmitting antenna connector | 1.5GHz | N-type |
| 2 | 5.2GHz transmitting antenna connector | 5.2GHz | N-type |
| 3 | 1.4GHz transmitting antenna connector | 1.4GHz | N-type |
| 4 | 840-930MHz transmitting antenna connector | 900MHz | N-type |
| 5 | GNSS satellite receiving antenna connector | GNSS | N-type |
| 6 | 5.8GHz transmitting antenna connector | 5.8GHz | N-type |
| 7 | 433MHz transmitting antenna connector | 433MHz | N-type |

| | | | |
|---|---|---|---|
| 8 | 1.2GHz transmitting antenna connector | 1.2GHz | N-type |
| 9 | 2.4GHz transmitting antenna connector | 2.4GHz | N-type |

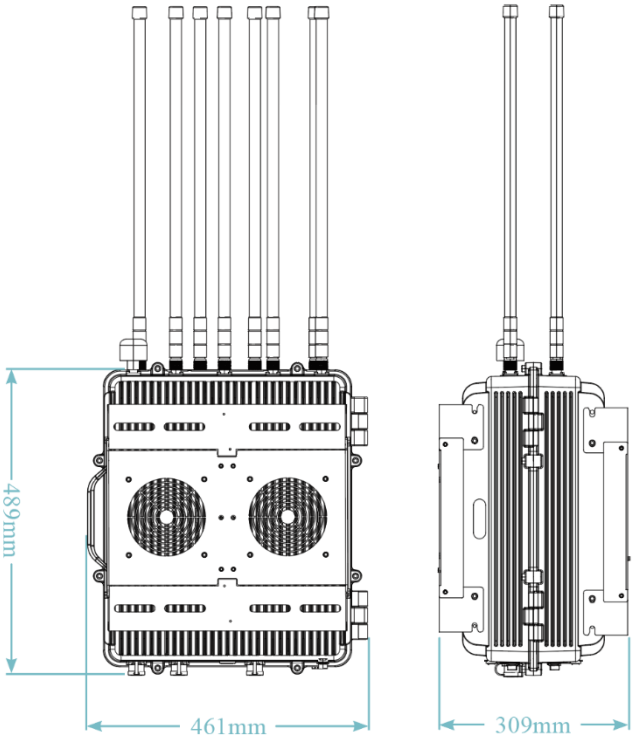



| Position | Description | Label | Connector Type |
|---|---|---|---|
| 1 | Ethernet port 1 | | RJ45 |
| 2 | Ethernet port 2 | G | Optical Fiber Connector |
| 3 | Power On/Off button | | — |
| 4 | Power connector (AC110V～240V) | | AC110V～240V aviation power connector |
| 5 | Fan connectors | FAN1 | 2 pin aviation connector |
| | | FAN2 | |

## 1.4 Mechanical Characteristics

| Item | Specification |
|---|---|
| **Size**(1) | |
| Length | 489mm |
| Width | 461mm |
| Thickness | 309mm |
| **Weight** | |
| Weight | 35kg |

(1) The data are of the main unit, including fans but excluding antennas.



# 2 Equipment Deployment Preparation

Choose a wide-view area to erect the device. First check the specifications and quantity of all parts and standard parts according to the equipment list, and then assemble them step by step according to the following installation steps.

## 2.1 Site Selection

The equipment is typically deployed outdoors. A comprehensive site survey must be conducted prior to installation and deployment. Site the equipment should pay attention to the following factors:

**Visibility environment:** Choose a flat, open highland or building rooftop, ensuring a 360° unobstructed view for the antenna placement.

**Electromagnetic environment:** Avoid electromagnetic interference zones such as microwave stations, radio transmission towers, and high-voltage power line crossings, as well as areas near glass curtain wall clusters and large metal structures (e.g., bridges, transmission towers).

**Natural environment:**

- Avoid the wind to reduce the equipment antenna wind load.
- When deploying in thunderstorm-prone areas, avoid locations susceptible to water accumulation and lightning strikes. Install a lightning rod for protection; its height must exceed the overall equipment height by at least 50 cm.

**Electrical Environment:** Avoid areas near electrified railways, base stations, or any other sources prone to signal interference.

**Infrastructure:** Ensure the site has mains power access and supports connection to public or dedicated communication networks.

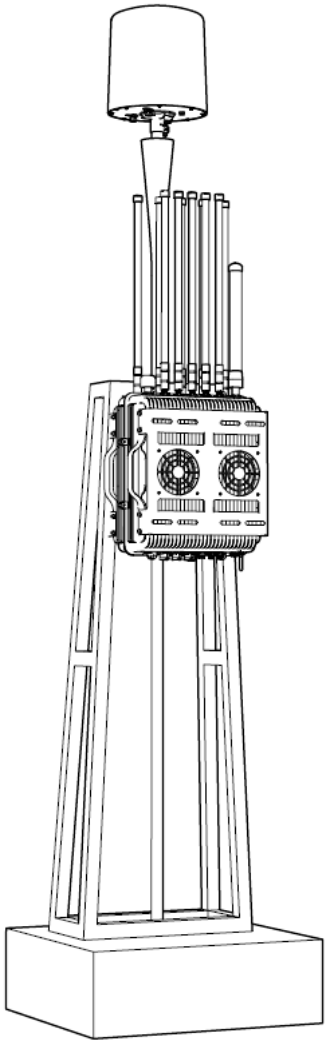
**Additional Requirements:** The deployment site must be legally designated for construction. The building structure or mounting bracket must have sufficient load-bearing capacity to meet the equipment’s weight requirements.

## 2.2 Installation Methods

It can be mounted on a pole or wall. Be aware of the surroundings and make sure there are no obvious obstructions or strong jamming devices in the area.

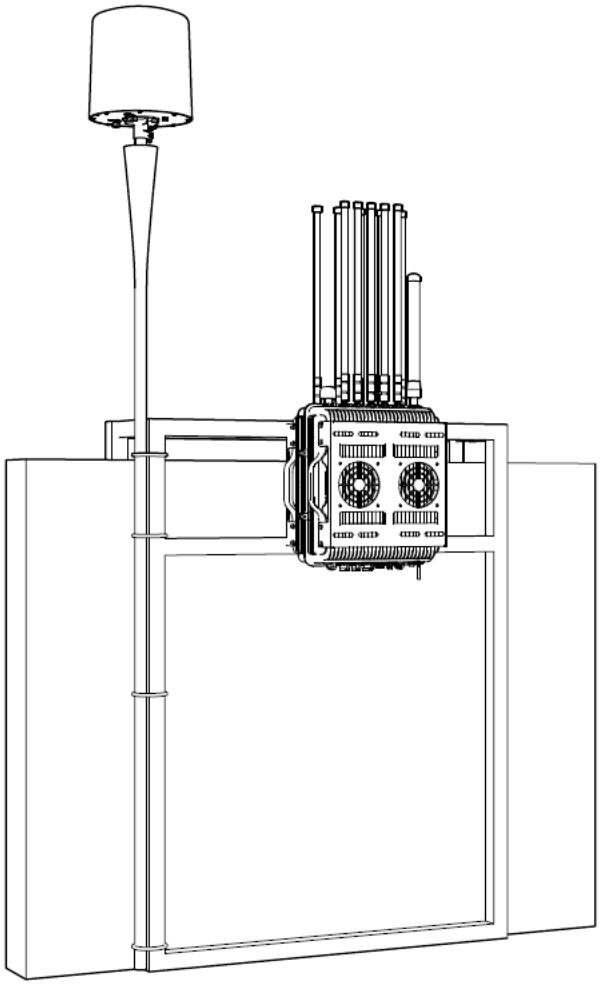
### Method 1: Ground Installation.

The equipment features an external mounting bracket on the back, which can be connected and secured to a prepared ground installation bracket using M10 bolts. The ground installation bracket should be firmly installed on the ground.



# Method 2: Wall Installation.

The equipment is connected and secured to a wall mounting bracket using bolts, and the wall mounting bracket is fixed to the wall using expansion anchors.

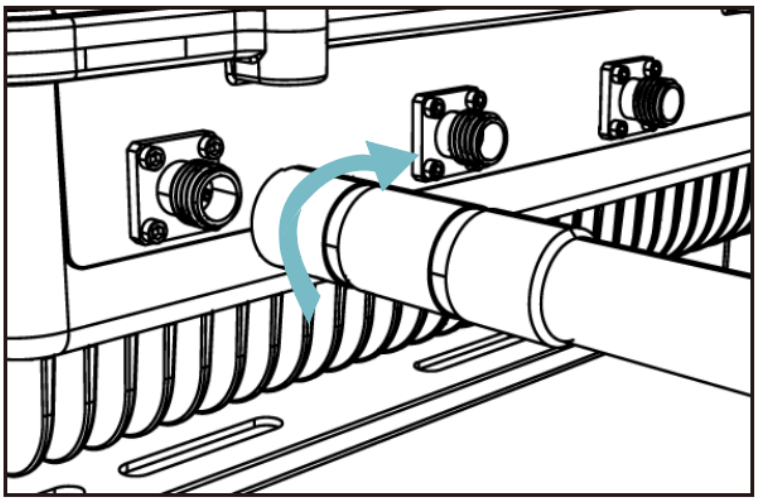


# 3 Deploy the Equipment

## 3.1 Connect Antennas

All antennas must be installed on the main unit according to the labels.

1. Tighten 8 transmitting antennas and 1 GNSS satellite receiving antenna onto the main unit one by one in a clockwise direction in accordance with the corresponding labels of main unit and antennas.



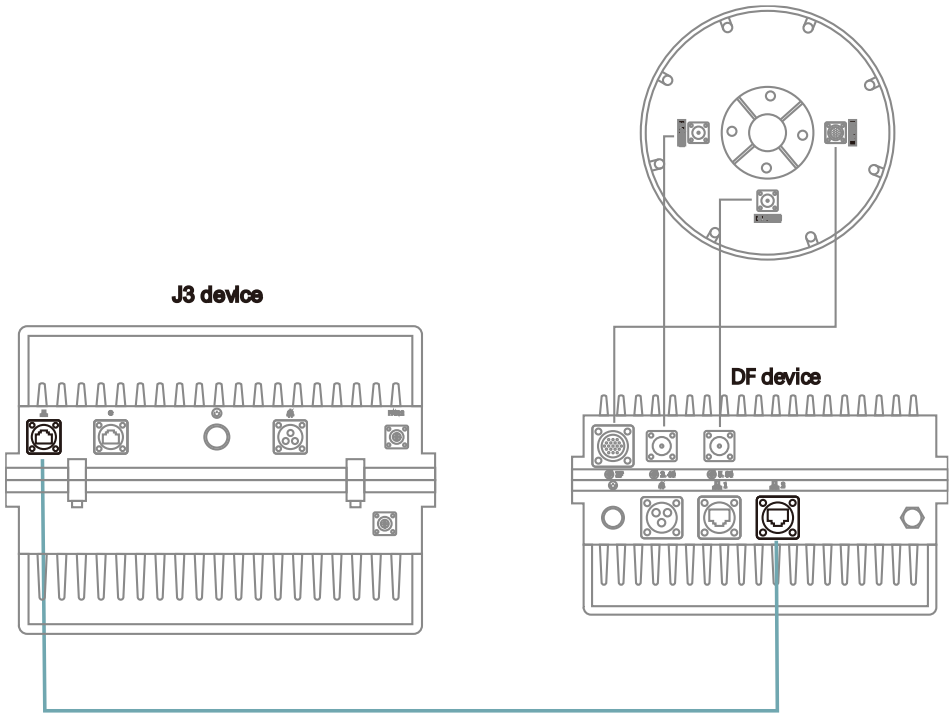
All antennas must be securely installed on the main unit before use. If any antenna is missing or damaged, do not operate the equipment; continued use will cause damage.

## 3.2 Connect with Detection Device

The J3 device requires integration with detection device to achieve drone detection and defense capabilities. The following steps demonstrate the connection procedure between the J3 and the DF device as an example.

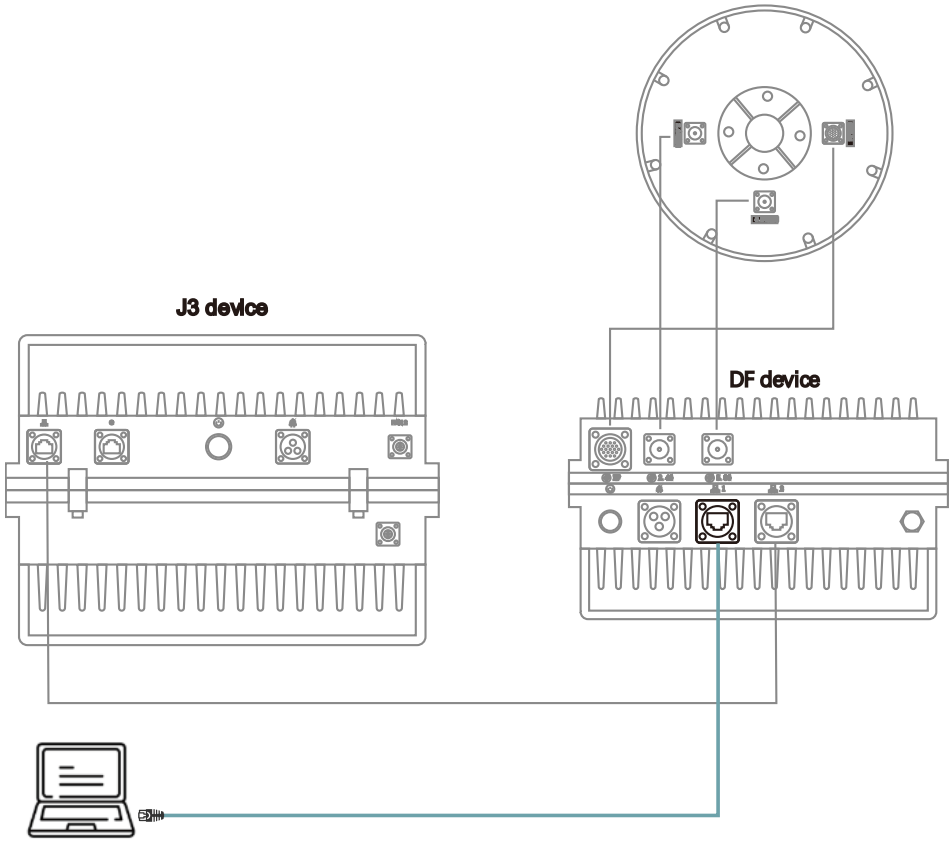
The DF device is fully deployed with all antennas, including the direction-finding antenna installed.

1. Connect the Ethernet port 2 on the DF device to the Ethernet port 1 on the J3 device using an ethernet cable.




2. Connect the Ethernet port 1 on the DF device to the control terminal using an ethernet cable.

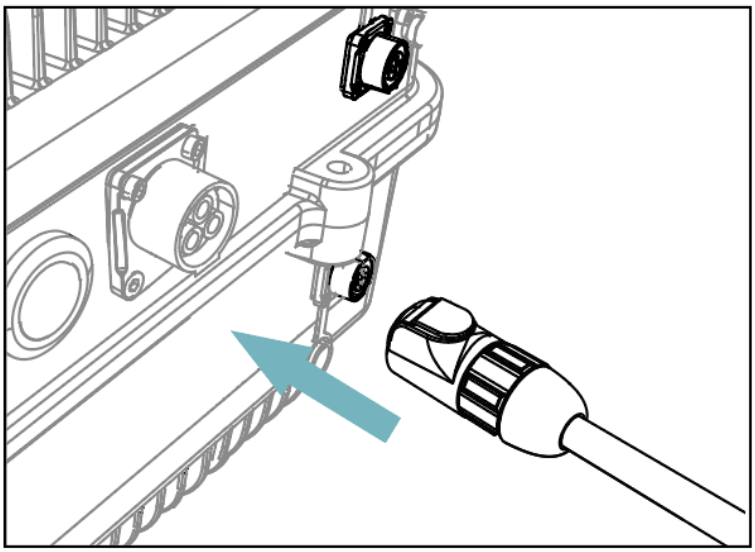
| | |
|---|---|
| ⓘ | Cover any unused Ethernet port with the waterproof plugs supplied on the device. |



## 3.3 Connect Fan

The J3 bracket is equipped with built-in cooling fans on both sides.

1. Connect each fan's power cable to the corresponding fan interface on the same side of the main unit.

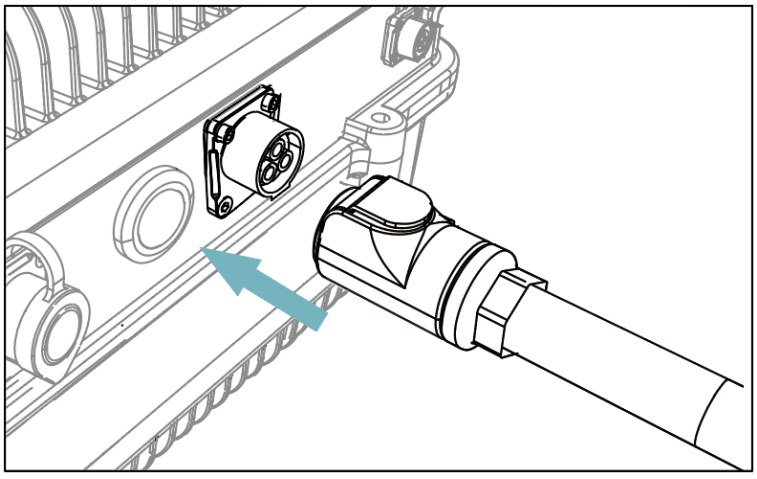


## 3.4 Connect Power Supply

Both the J3 and the DF device can be connected to 110V-220V AC power via power cable using either fixed power supply or UPS.

> ⚠ The J3 and the DF device must have their antennas installed before power on. Otherwise, the device may be damaged.

1. Connect the input end of the power cable to the fixed power supply and insert the output end into the device’s power connector. The power connector features a snap-fit design, apply steady pressure until you hear an audible click, confirming a secure connection.



# 4 Drone Defense Software Platform

Drone defense software platform, which integrates situational awareness, information display, decision-making assistance, command and control. It supports browser access and control of other devices on the LAN, and supports multi-screen and multi-device monitoring.

After both host devices are powered on, the control terminal connected to Ethernet port 1 of DF device can proceed with system login.

## 4.1 Log in to the System

### Configure the Network

Before logging into the system, it is necessary to configure the network settings of the drone defense software platform. The IP address should be set within the 192.168.100.x subnet, which is the same subnet as the default access IP of the system: 192.168.100.100.

1. Configure the IP subnet to 192.168.100.x according to the system platform, e.g., Windows, Linux, or macOS.

| | |
|---|---|
| | Avoid setting the IP address to 192.168.100.100 or the default IP address 192.178.1.101 of J3, as this will cause a conflict. |

### Log in to the System

1. Open a browser and enter the device's IP address https://192.168.100.100 to access the login page.

| | |
|---|---|
| | Google Chrome is recommended for use. |

2. Enter the system account and password, drag the verification slider to verify, and then click the “Sign in” to enter the main interface of the system.

| | |
|---|---|
| Account: | admin |
| Password: | lzno1 |

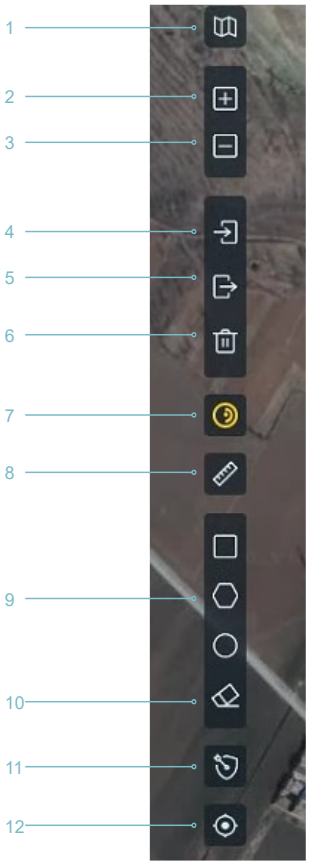
## 4.2 Main Interface

The main interface is distributed in three functional areas.

1. Operation menu area
2. Information display area
3. Function display area

# Operation Menu Area

The operation menu area includes options such as map mode switch and defense-zone settings.



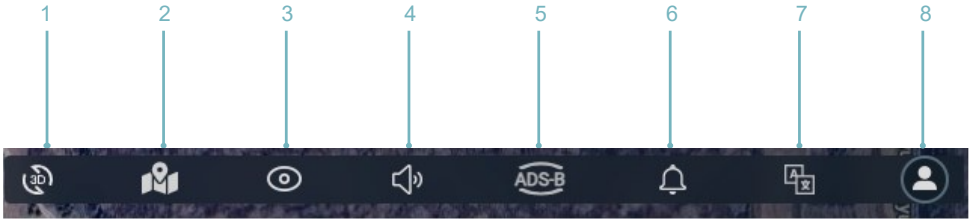

| | | |
|---|---|---|
| 1 | Map mode switch | Switch between Google satellite and Google vector. |
| 2 | Zoom In | Zoom In the map. |
| 3 | Zoom Out | Zoom Out the map. |
| 4 | Import map | Import offline map files into the system. When the network disconnected, it will automatically switch to the loaded offline maps.<br>The offline map file must be named and formatted as **mapTiles.db**. |
| 5 | Export map | Export the offline map files that have been imported into the system. View the exported map files in the browser's download list. |

| | |
|---|---|
| 6 Clear offline map files | Delete the imported offline map files. |
| 7 Set center point | Sets the center point coordinates for networking. Not applicable for single-device operation. |
| 8 Measuring distance | Measure the distance and angle between two points on the map, allowing for the measurement of distances and angles between multiple endpoint positions and a starting point. |
| 9 Draw defense zone or warning zone | Set Defense Zone/Warning Zone on the Map.<br>**Defense Zone:** Once set, the defense zone appears as a red inner circle. If a drone enters this zone, it will be highlighted in orange, and audible/visual alarms will activate. When unattended mode is enabled, unauthorized drones entering the defense zone will be automatically intercepted, repelled, or forced to land.<br>**Warning Zone:** Once set, the warning zone appears as a blue inner circle. If a drone enters this zone, it will be highlighted in orange, and audible/visual alarms will activate. Unauthorized drones entering the warning zone will trigger continuous alerts while their position and flight path are monitored. But no active interference will be applied.<br> The minimum allowable area for drawing defense/warning zones is 100 square meters. |
| 10 Eraser Defense Zone | Delete the defense zone or warning zone drawn on the map. |
| 11 Locate the air defense zone | If the device moves too far and loses the defense/warning zone, perform rapid repositioning. |
| 12 Return to center | Return to the center point. |

## Information Display Area

The information display area includes options such as hiding/displaying the menu bar of the main interface, volume, notification switch, language switch, system logon/logoff and other operations.

In addition, this area is mainly responsible for the real-time detection information display and control functions of drones, which can display the number of current detection and historical detection drones, as well as the detailed information of currently detected drones.




| | |
|---|---|
| 1 3D Map | Switch between 3D map view and 2D map view. |
| 2 Historical Drones Detection Setting | Display the historical drone-detection locations on the map and marked with yellow. The date range can be configured by start time and end time. |
| 3 Hide/Show panel | Hide or show the detection area, function area, and map area of the interface. |
| 4 Sound settings | Adjust the alarm volume. |
| 5 ADS-B | Used to receive civil aviation signals transmitted by aircraft, including flight route and schedule information. |
| 6 Notifications | Display device status notifications. |
| 7 Change language | Change system language. |
| 8 Account login | Account login/logout. |

## Function Display Area

The function display area includes options such as checking the events, checking the whitelist, checking the statistic, checking the device status and other operations.

Click the button to expand the function display area menu. Click the same button again to hide the menu.

| | | |
|---|---|---|
| 1 | Events | The Drone Events list shows drone details such as type, ID, detection time, duration, and frequency. It supports sorting, time-based expansion, history replay, export drone events, clear drone events on the main screen. |
| 2 | Advanced | Includes the unknown UAV WiFi detection, Custom Detectors, Custom Models module. |
| 3 | Black/White | Drones added to the blacklist will be flagged with an alert once they enter the defense zone. Drones on the whitelist will not trigger any alarm when they enter defense zone.<br><br>Whitelist/blacklist exports are saved in UTF-8 format. View the exported files in the browser's Downloads list. |
| 4 | Statistics | The Drone Statistical Report includes Incidents/Drones, Most Seen Drone Brands, Common UAV, Incident Trends and Critical Incidents. It supports date range configured by start time and end time, and export PDF of the statistics. |
| 5 | Devices | The device management window displays the operational status information of controller, engine, sensors and defender.<br>● Controller: Display the information such as operation status, and detection bands.<br>● Engine: Display the information such as operation status, GPU and CPU information, and version.<br>● Sensors: Display the information such as operation status, detection bands, and version of the two sensors.<br>● Defender: Display the information such as operation status, faults, and version. |

| | | |
|---|---|---|
| 6 | Version | Display the version information of UI version, cm, engine, sensor, defender. |
| 7 | Settings | Modify passwords and do user management, such as add, edit and delete. |
| 8 | Function display area | The functional display area primarily shows the Spectrum, Incident Trends, and Most Seen Drone Brands. The spectrum feature visualizes signals currently detected by the device as a spectrum. |

## 4.3 Check Detection Information

When a drone is detected, the system triggers an automatic alarm.

1. View the detected drone model information on the main interface, while an intrusion alert message pops up at the top of the screen.
2. In Information Display Area, it displays the position and direction of the drone. Additionally, the drone model, electronic ID and approximate location information are marked on the electronic map in the main interface.

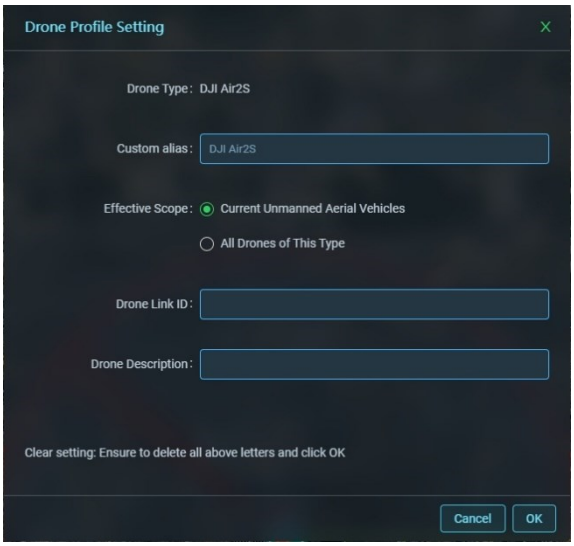
### Add to/Delete from Whitelist

Drones added to the whitelist will not trigger any alarm when they entering the defense zone.

1. Select a drone.
   a) Click **AddWhitelist** button to add the drone to whitelist.
   b) Click **DeleteWhitelist** button to delete the drone from whitelist.

## Set Drone Profile

1. Select a drone. Click button and select **Profile**.
2. On the Drone Profile Setting page, configure the Custom alias, Effective scope, Drone Link ID, and Drone Description.




# 4.4 Drone Jamming

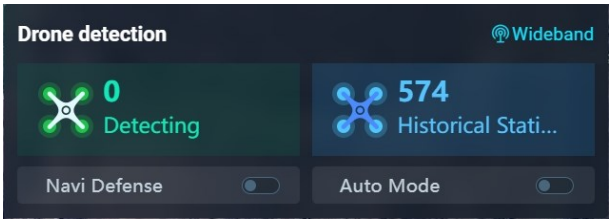
The device supports precise jamming and wideband jamming.

## Set Precise Jamming

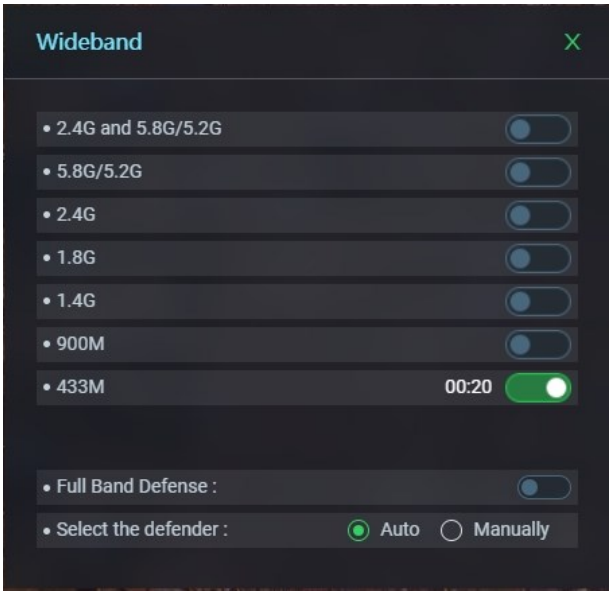
1. In Information Display Area, select a drone and click **Precision** button to start precise jamming.
2. During precise jamming, click **Cancel** button to cancel the precise jamming.

## Set Wideband Jamming

1. In Information Display Area, click **Wideband** button, and enters Wideband setting page.




2. Slide the button to activate the wideband jamming for this frequency band.

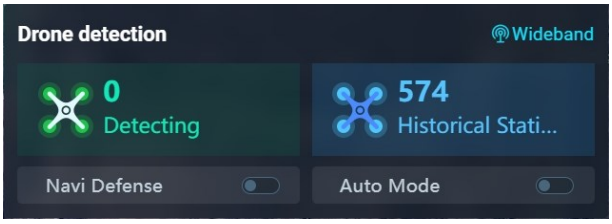



3. During wideband jamming, click **Cancel** button to cancel the wideband jamming.

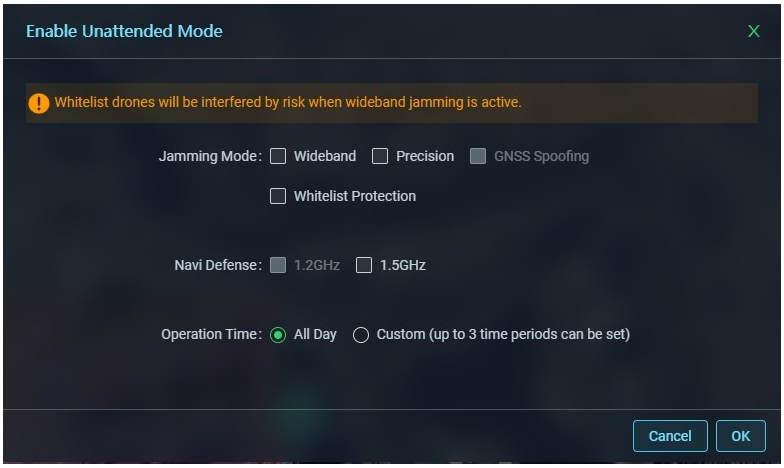
## 4.5 Enable Unattended Function

In unattended mode, the system automatically identifies and filters drones on the whitelist upon detection. For blacklisted drones, it initiates wideband jamming or precise jamming. The countermeasures will automatically cease once the alarm is no longer triggered.

1. In Information Display Area, toggle the switch of **Auto Mode** to enter the Autonomous Defense Option Confirm page.




2. In the page, set Jamming Mode, Navi Defense, and Operation time.




3. Click **OK** button to enable unattended function.

## 4.6 Check the Events

1. In Function Display area, click **Events**, view the drone events.

This feature allows one-click expand/collapse of the “Incident Trends” panel on the main interface.

2. Click **Export Drone Events** button to export drone events.

## 4.7 Mark Danger WiFi Drones

The device can display the drone-like WiFi signals detected in the current environment and allow users to mark them.

1. In Function Display area, click **Advanced**.
2. Select Unknown WiFi panel to enter the WiFi list.

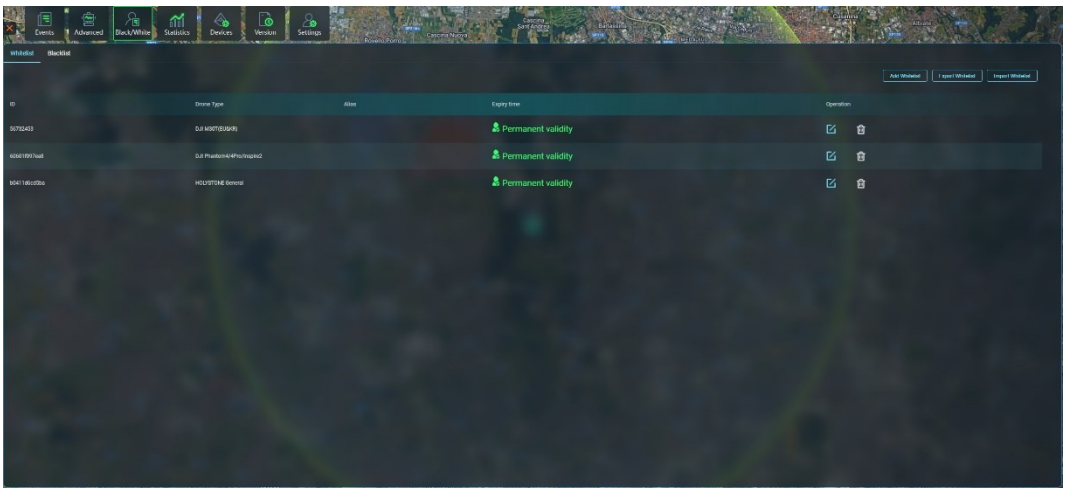
3. Mark the WiFi signal.

a) Users may mark an identified non-drone WiFi signal (e.g., a common wireless hotspot) as “Safe.” Once marked, the system will ignore this signal and not trigger alarms.

b) If a WiFi signal is confirmed to originate from a drone, users can mark it as “Danger”. After marking, the system will trigger an alarm whenever this signal is detected.

## 4.8 Manage the Whitelist/Blacklist

Drones added to the blacklist will trigger visual alerts when entering the defense zone, while whitelisted drones will not trigger any alarm when they appear.




### Export Whitelist/Blacklist

1. In Function Display area, click **Black/White**.
2. Click **Export Whitelist/Blacklist** button to export whitelist or blacklist.

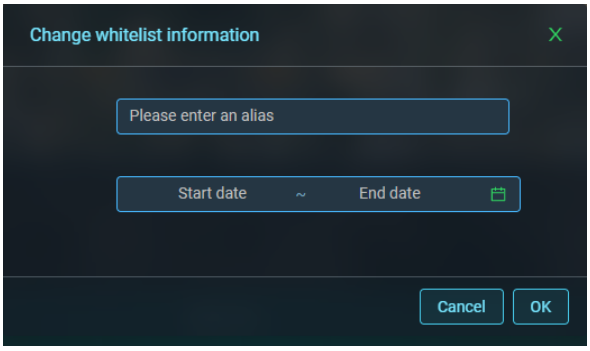
Export format is UTF-8. View exported lists in the browser’s download list.

### Add Whitelist/Blacklist

1. In Function Display area, click **Black/White**.
2. Click **Add Whitelist/Add Blacklist** button, enter the ID, Drone Type, Alias, set Effective time, then click to add.

## Update Whitelist/Blacklist

1. In Function Display area, click **Black/White**.
2. Select a list formation to be updated, click button, update information.
   a) For whitelist, update alias, and effective time range.




   b) For blacklist, update alias.

## Delete Whitelist/Blacklist

1. In Function Display area, click **Black/White**.
2. Select a whitelist or blacklist to be deleted, click button and information will be deleted directly.

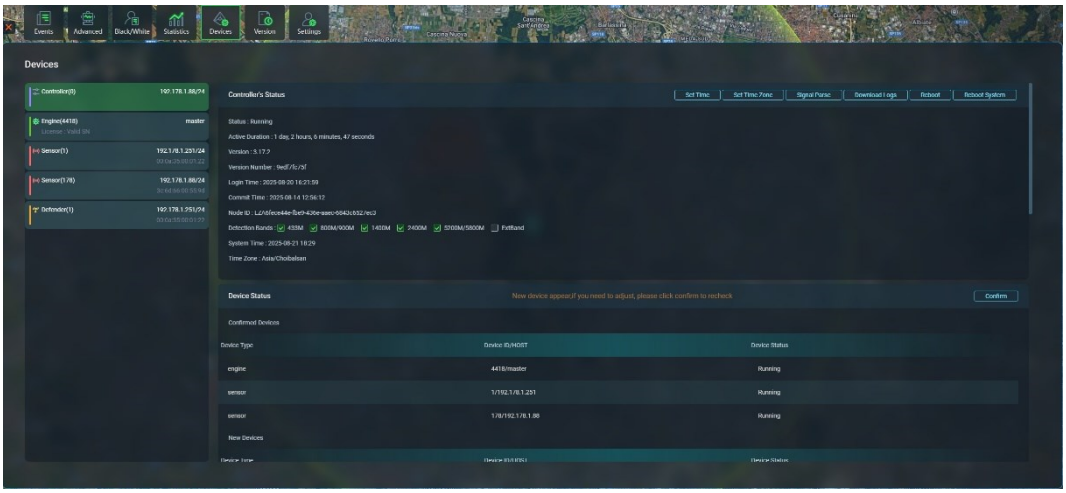
# 4.9 Check the Statistic Report

1. In Function Display area, click **Statistics**. View the drone event statistics report.

2. Click **Export PDF**, set the time range and export the statistical report in PDF format.

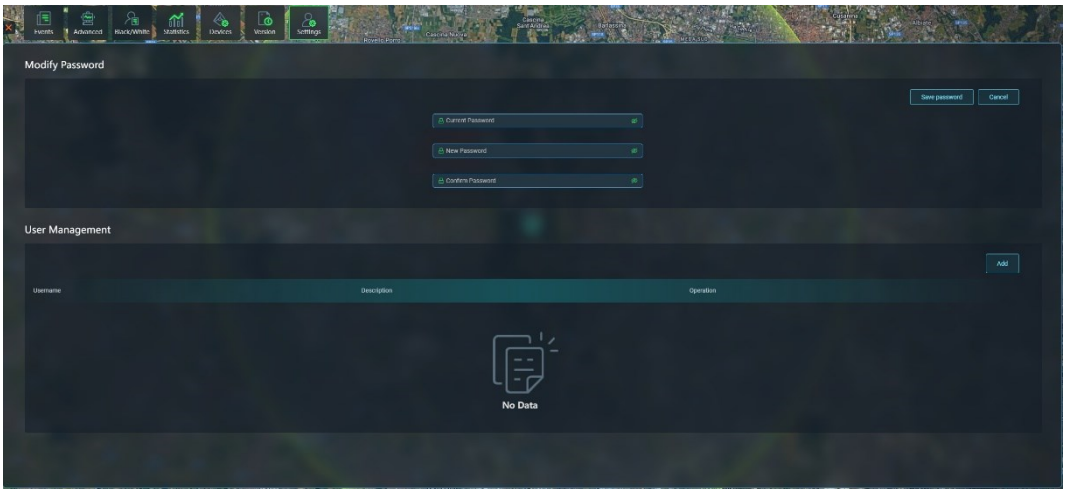
## 4.10 Check the Device Status

1. In Function Display area, click **Devices**. View the information of Controller, Engine, Sensors and Defender.




## 4.11 Change Password

1. In Function Display area, click **Settings**.



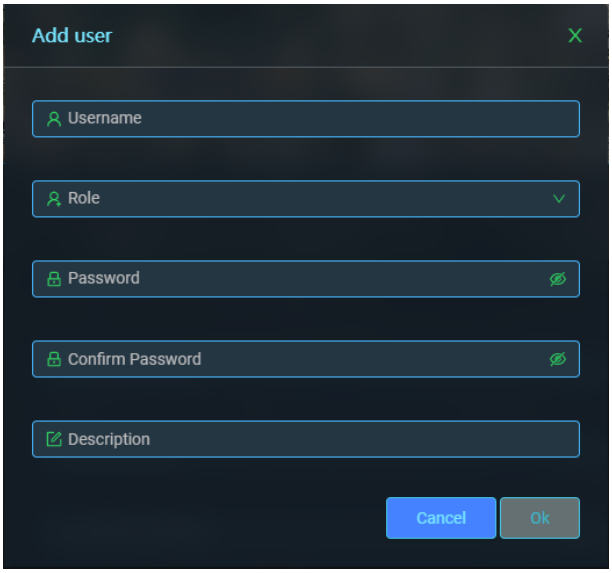

2. Enter the current password and the new password, then click **Save Password** button to set the new password.

## 4.12 Manage Users

This functionality is restricted to Admin accounts for user management. Normal accounts do not have these permissions.

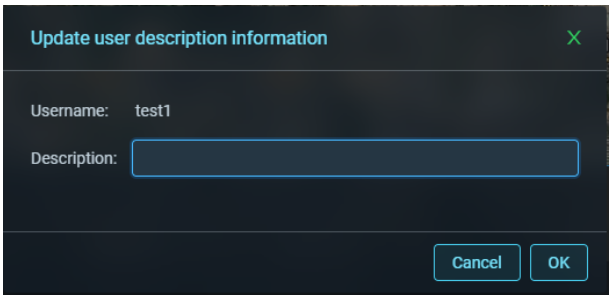
# Add Users

1. In Function Display area, click **Settings**.
2. Click **Add** button, enter the new user's username, role, password, and description information, then click "OK" to add the new user.




# Update User Description Information

1. In Function Display area, click **Settings**.
2. Select a user to be updated, click **Update** button, update the user's description information.




# Delete User

1. In Function Display area, click **Settings**.
2. Select a user to be deleted, click **Delete** button, click **Confirm** to delete the user.

# 5 Equipment Maintenance

To ensure stable operation of the equipment, please comply with the following maintenance specifications.

## 5.1 Routine Maintenance

| Maintenance Type | Maintenance Method |
|---|---|
| Interface protection | Seal unused interfaces with protective covers. |
| Cable maintenance | ● Do not replace antennas without authorization after deployment.<br>● Ensure cables and interfaces are fully engaged and securely locked.<br>● Immediately replace any feeder/power/Ethernet cables with damaged jackets or exposed wires.<br>● Ensure plug pins are not bent or damaged. |
| Power inspection | Verify that the device is powered normally. |

## 5.2 Basic Troubleshooting

| Fault Type | Troubleshooting Method |
|---|---|
| Power-related fault | ● Restart the power switch, boot the server, and launch the related services.<br>● Power off the device, wait for 30 seconds, and then restart it. |
| Network disconnection | ● Use the *ping* command to test connectivity between the device and the server.<br>● Unplug and reconnect the network cable, then verify that the port indicator light is on and stable. |
| System Process | Log in to the "Device" interface to check the process status of the |

| | |
|---|---|
| Exception | controller, engine, and sensors. |

If the issue persists, contact our technical support team.

Unauthorized personnel or non-designated maintenance personnel are prohibited from disassembling the chassis.

# 6 Packaging, Transportation and Storage

The equipment shall comply with the following requirements for packaging, transportation, and storage:

## 6.1 Packaging

The packing boxes shall be moisture-proof and shock-proof, and contain the following items:

- Delivery list
- Product Inspection Certificate
- User manual.

## 6.2 Transportation

In the process of transportation, avoid throwing, sun and rain, avoid mixing corrosive substances.

## 6.3 Storage

The storage shall meet the following requirements:

- Products should be stored in a cool, ventilated, dry warehouse.
- Do not put together with oil, away from heat sources.
- Stacking should be 20cm from the ground and 20cm from the wall.